

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, :

Plaintiff, :

-v.- :

OLEKSANDR DOROZHKO :

Defendant, :

Case No. 07 CIV 9606 (NRB)

POSTHEARING MEMORANDUM OF LAW
IN SUPPORT OF
PLAINTIFF SECURITIES AND EXCHANGE COMMISSION'S
MOTION FOR PRELIMINARY INJUNCTION AND OTHER EQUITABLE RELIEF
AND IN
OPPOSITION TO DEFENDANT DOROZHKO'S MOTION TO DISMISS

December 5, 2007

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
INTRODUCTION.....	1
I. RELEVANT FACTS AND PROCEDURAL HISTORY	1
II. RELEVANT PORTIONS OF THE STATUTE AND RULE	7
III. DEFENDANT DOROZHKO EMPLOYED THE FRAUDULENT AND DECEPTIVE DEVICE OF “HACKING” TO STEAL IMS HEALTH’S MATERIAL NONPUBLIC INFORMATION AND TO PROFITEER THEREON IN SECURITIES TRADING	8
A. Computer Hacking Involves Fraud or Deceit As Proscribed By Section 10(b) and Exchange Act Rule 10b-5.....	8
B. Established Case Law Supports The SEC’s Position That Theft Of Material Nonpublic Information By Hacking “In Connection With” Securities Trading Is Within The Purview of Section 10(b) And Exchange Act Rule 10b-5	11
IV. SEC’S ACTION AGAINST DEFENDANT DOROZHKO IS CONSISTANT WITH ESTABLISHED LEGAL PRINCIPLES UNDER SECTION 10(b) AND EXCHANGE ACT RULE 10b-5	12
A. Section 10(b) Addresses Fraud Accomplished Through Hacking.....	12
B. <u>Chiarella</u> Is Not Inconsistent with Obtaining Information by Deception	13
C. Even Without the Breach of a Duty, Hacking Is Contemplated as a Violation of Section 10(b) and Exchange Act 10b-5.....	14
V. APPLYING SECTION 10(b) AND EXCHANGE ACT RULE 10b-5 TO DEFENDANT DOROZHKO’S CONDUCT COMPORTS WITH CONGRESSIONAL INTENT AND PUBLIC POLICY	17
VI. CONCLUSION.....	21

TABLE OF AUTHORITIES

FEDERAL CASES

<u>Blueport Co., LLP v. U.S.</u> , 76 Fed. Cl. 702 (Fed. Cl. 2007)	9
<u>Chiarella v. U.S.</u> , 445 U.S. 222 (1980), <u>aff'd by an equally divided court</u> , 484 U.S. 19 (1987).....	12, 14, 19
<u>Dirks v. SEC</u> , 463 U.S. 646 (1983).....	14
<u>Hammerschmidt v. United States</u> , 265 U.S. 182 (1924).....	15
<u>Kemp v. American Telephone & Telegraph Co.</u> , 393 F.3d 1354 (11th Cir. 2004)	12
<u>McNally v. United States</u> , 483 U.S. 350 (1987)	15
<u>Nugent v. Ashcroft</u> , 367 F.3d 162 (3rd Cir. 2004)	12
<u>Physicians Interactive v. Lathian System, Inc.</u> , 2003 U.S. Dist. LEXIS 22868 (E.D.Va. Dec. 5, 2003)	9, 10
<u>SEC v. Blue Bottle Ltd.</u> , 07 CIV 01-CV-1380 (CSH)(S.D.N.Y. Feb 26, 2007)	16
<u>SEC v. Capital Gains Research Bureau</u> , 375 U.S. 180 (1963)	19
<u>SEC v. Cherif</u> , 933 F.2d 403 (7th Cir. 1991).....	15
<u>SEC v. Lohmus Haavel & Viisemann, et al.</u> , 05 CV 9259 (RWS) (S.D.N.Y. Nov. 1, 2005)	10, 16
<u>SEC v. Maio</u> , 51 F.3d 623 (7th Cir. 1995).....	8
<u>SEC v. Materia</u> , 745 F.2d 197 (2d Cir. 1984).....	15, 21
<u>SEC v. Rocklage</u> , 470 F.3d 1 (1st Cir. 2006)	14
<u>State Wide Photocopy Corp. v. Tokai Finance Svcs., Inc.</u> , 909 F. Supp. 137 (S.D.N.Y. Aug. 3, 1995)	9
<u>Travelers Intern., A.G. v. Trans World Airlines, Inc.</u> , 41 F.3d 1570 (2d Cir. 1994).....	17

<u>U.S. v. Falcone</u> , 257 F.3d 226 (2d Cir. 2001).....	15
<u>U.S. v. Carpenter</u> , 791 F.2d 1024 (2d Cir. 1986) <u>aff'd by equally divided court</u> , 484 U.S.19 (1987).....	7, 15, 18, 19
<u>U.S. v. O'Hagan</u> , 521 U.S. 642 (1997).....	7, 11, 12, 13, 21

STATE CASES

<u>Briggs v. State</u> , 704 A.2d 904 (Md. 1998).....	7
---	---

FEDERAL STATUTES

Exchange Act of 1934	
Section 10(b), [15 U.S.C. § 78j(b)].....	7
Rule 10b-5, [17 C.F.R. § 240.10b-5]	7
18 U.S.C. §1030.....	10
18 U.S.C. § 1030(a)(4)	10
18 U.S.C. § 1341	10
18 U.S.C. § 1343.....	10
Insider Trading Sanctions Act of 1984, P.L. No. 98-376, 98 Stat. 1264	18

FEDERAL RULES OF CIVIL PROCEDURE

Rule 12b(6)	5
-------------------	---

LEGISLATIVE REFERENCES

H.R. 8720	17
H.R. 9233, 73d Cong., 2d Sess	19
H.R. Rep. No. 98-355, 98th Cong., 1st Sess. 3, 4 (1983), <u>reprinted in</u> [1984] U.S. Code Cong. & Admin. News 2274	18
Hearings on H.R. 7852.....	17
S. Rep. No. 792, 73d Cong., 2d Sess., 6 (1934).....	20

MISCELLANEOUS

18 <u>Insider Trading Regulation, Enforcement, and Prevention</u> § 6:14 (Apr. 2007)	16
Donald C. Langevoort, 18 <u>Insider Trading Regulation, Enforcement, and Prevention</u> § 6:14 (Apr. 2007)	16
Restatement (Second) of Contracts § 205 (date)	17
Robert A. Prentice, "The Internet and Its Challenges for the Future of Insider Trading Regulation," 12 <u>Harvard Journal of Law & Technology</u> 263, 298-307 (1999)	17, 22
Victor Brudney, <u>Insiders, Outsiders, and Informational Advantages Under the Federal Securities Laws</u> , 93 Harv. L. Rev. 322, 356 (1979).....	21

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, :

Plaintiff, :

-v.- :

OLEKSANDR DOROZHKO :

Defendant, :

Case No. 07 CIV 9606 (NRB)

**POSTHEARING MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF
SECURITIES AND EXCHANGE COMMISSION'S MOTION FOR PRELIMINARY
INJUNCTION AND OTHER EQUITABLE RELIEF AND OPPOSITION TO
DEFENDANT DOROZHKO'S MOTION TO DISMISS**

Plaintiff Securities and Exchange Commission (the "SEC"), having filed a Complaint naming Oleksandr Dorozhko ("Dorozhko") as defendant, respectfully submits this Posthearing Memorandum of Law in Support of Plaintiff Securities and Exchange Commission's Motion for Preliminary Injunction and Other Equitable Relief and in Opposition to Defendant Dorozhko's Motion to Dismiss. At a hearing held on November 28, 2007, the Court requested that the SEC to submit a brief further supporting the SEC's position that the type of conduct presented here, the secret and deceptive hacking into a private computer system for purposes of obtaining material nonpublic information for use in securities trading, is a violation of Section 10(b) of the Securities Exchange Act of 1934 ("Exchange Act") and Rule 10b-5. (Hr'g Tr. at 134).

I. Relevant Facts and Procedural History

Defendant Dorozhko has declined to provide any evidence in this case, based on Fifth Amendment privileges. (Gumagay Decl. ¶ 7 and Ex. F). It appears that he is a self-employed Ukrainian national residing in Uzhgorod, Ukraine. (Gumagay Decl. ¶ 3 and Ex. B; Gumagay

Decl. ¶ 4 and Ex. C). In his application to open an account at Interactive Brokers LLC (“Interactive Brokers”), Defendant Dorozhko represented that he had an annual net income of approximately \$45,000-\$50,000 and claimed a net worth of between \$100,000-\$250,000. (Gumagay Decl. ¶ 4 and Ex. C). On or about October 4, 2007, Defendant Dorozhko wire transferred \$42,500 to Interactive Brokers to open an online trading account. (Gumagay Decl. ¶ 4-5 and Ex. C-D).

On October 17, 2007, IMS Health Incorporated (“IMS Health”), a public company headquartered in Norwalk, CT, prepared for the announcement of its third quarter earnings results, which was scheduled to be released at 5:00 p.m. (after the close of the trading markets) that day. (Fox Decl. ¶ 4). IMS Health, its employees and its agents took very substantial steps to maintain the confidentiality of the earnings information to ensure that no one could access and exploit for personal benefit the information prior to its public release. (*Id.*). Such confidentiality was especially important, because IMS Health was about to announce earnings well below analyst consensus estimates for the third quarter of IMS Health’s 2007 fiscal year and there were no media/analyst reports at the time anticipating negative earnings. (*Id.*). For several years, Thomson Financial has “hosted” IMS Health’s investor relations website and provided secure webcasting and audiocasting services for IMS Health’s public release of earnings information. (Hr’g Tr. at 23, 28). IMS Health used Thomson Financial for the October 17th announcement. (Fox Decl. ¶ 6). IMS Health routinely publicized the date, time and Internet location for an IMS Health conference call - web cast. (Hr’g Tr. at 69). Thus, as early as on October 9, several days prior to the October 17 announcement, IMS Health publicly disclosed that it would announce its third quarter earnings on October 17th at 5:00 p.m. (EST) on the IMS Health website at Thomson Financial. (Dorozhko Ex. A). Thomson Financial, seeking to assure confidentiality of

client information and to preserve its own reputation for standards of high security, had elaborate multi-layered procedures in place to block pre-release access to information such as IMS Health's third quarter results – by anyone except authorized IMS Health and Thomson Financial personnel. (Hr'g Tr. at 26-27, 51-52).

At 8:06 a.m. (EST) on October 17, a computer hacker, who the SEC alleges is Defendant Dorozhko, began probing the IMS Health website at Thomson Financial for weaknesses in its security to illegally access IMS Health information before it went public.¹ (Ex. SEC 2; Hr'g Tr. at 35) Since Thomson Financial had not yet received any IMS Health information, this effort was unsuccessful. (Ex. SEC 2; Hr'g Tr. at 36) All Defendant Dorozhko saw was the publicly available "Event Detail" – noting merely the scheduling of the IMS Health earnings announcement. (Ex. SEC 2; Hr'g Tr. at 36, 48) This probe occurred nearly nine hours before the time scheduled for the announcement – at a time when one would expect that IMS Health earnings information, if present, would have been guarded by Thomson Financial's security system. (Ex. SEC 2).

Three times thereafter, at 12:10 p.m., at 12:51 p.m., and at 1:52 p.m., Defendant Dorozhko returned and probed to determine if Thomson Financial had received the nonpublic IMS Health information. Thomson Financial had not. (Ex. SEC 2; Hr'g Tr. at 38).

At 2:01 p.m. on October 17, IMS Health sent Thomson Financial certain slides for IMS Health's conference call and web cast with investors scheduled for 5:00 p.m.. (Id.; Hr'g Tr. at 28-29 and Ex. SEC 1). The slides contained very material and highly confidential information

¹ Direct evidence that Dorozhko is this "hacker" has been concealed by layers technological anonymity and, with "spoofing", may hide in the "cyber shadows" for some time. However, the compelling circumstantial evidence that only after the hacking succeeded, and only within 30 minutes after retrieving the IMS Health Corporate Information, did Defendant Dorozhko bet "the ranch" in an all-or-nothing gamble that IMS Health shares would suffer an unprecedented price decline within two days. When coupled with the negative inferences that may be drawn from Dorozhko's invocation of Fifth Amendment privileges, there is ample justification to conclude that Defendant Dorozhko was the computer hacker.

concerning IMS Health's third quarter earnings for fiscal year 2007. (Fox Decl. ¶ 6; Hr'g Tr. at 28-29 and Ex. SEC 1, p. 9). After receiving the slides, Thomson Financial prepared them for the 5:00 p.m. IMS Health presentation and at approximately 2:08 p.m. Thomson Financial uploaded them to a secure proprietary database to be posted to IMS Health's website at a later time. (Hr'g Tr. at 29) IMS Health had every expectation that the slides sent to Thomson Financial would remain confidential until publicly released. (Fox Decl. ¶ 6). Thomson Financial had the same expectation and had established very complex procedures to provide such security. (Hr'g Tr. at 24, 49-51).

However, at 2:15.01 p.m., within minutes after the slides were uploaded, the Hacker, again probed the Thomson Financial computer network to see if the IMS Health earnings information had been received, and this time learned that Thomson Financial had the IMS Health information.² (Hr'g Tr. at 37 and Ex. SEC 2). Within 27 seconds, starting at 2:15:28 p.m., Defendant deceived the Thomson Financial security system into letting him gain "illegal" access (as characterized by Mr. Mathias) to the confidential IMS Health information, and by 2:18.43 p.m., The Hacker had taken copies of all the IMS Health earnings information. (Hr'g Tr. at 32 to 38 and Ex. SEC 2).

It is not surprising that within one-half hour after getting the confidential IMS Health information, starting at 2:52 p.m., Defendant Dorozhko began a very aggressive campaign to capture as many puts on IMS Health shares offering the greatest post-announcement profit from the funds he had available to invest. (Hr'g Tr. at 93;). For example, his first order was for 100

² Direct evidence that Dorozhko is this "hacker" has been concealed by layers technological anonymity and, with "spoofing", may hide in the "cyber shadows" for some time. However, the compelling circumstantial evidence that only after the hacking succeeded, and only within 30 minutes after retrieving the IMS Health Corporate Information, did Defendant Dorozhko bet "the ranch" in an all-or-nothing gamble that IMS Health shares would suffer an unprecedented price decline within two days. When coupled with the negative inferences that may be drawn from Dorozhko's invocation of Fifth Amendment privileges, there is ample justification to conclude that Defendant Dorozhko was the computer hacker.

Oct 25 calls. (Ward Decl. ¶ 10 and Ex. 5) These options would expire on Saturday, so Defendant Dorozhko could only make a profit if the price of IMS Health stock dropped more than 20% in the next two days – a decline that was unprecedented for IMS Health stock. (Glascoe ¶ 11, 12 and 13) Apparently unable to get his order filled, within seconds, Defendant Dorozhko cancelled this order and seconds later he doubled the premium he would pay for these options. (Ward Decl. ¶10 and Ex. 5) During the next 15 minutes, Dorozhko feverishly tried to accumulate October puts, six times cancelling all or part of open orders, and about six times revising his orders or raising his bids. (Ward Decl. ¶10; Ward Ex. 5) By 3:06 p.m., Defendant Dorozhko succeeded in garnering 300 Oct 25 and 330 Oct 30 IMS Health put options and invested \$41,670.90 - nearly all the money available in his account, a sum about equal to his income for one year and one-fifth his net worth. The risk to his investment was enormous. (Glascoe Decl. ¶ 15) If the price of IMS Health stock did not drop below the strike price (plus the premiums he paid) in two days, then he would lose everything he invested – approximately one year of his income and nearly one-fifth of his net worth. (Hr’g Tr at 111-113). Defendant Dorozhko’s purchases were also exceptional in comparison to the market – they represented almost 90% of all purchases in those option series between September 4, 2007, and October 17, 2007. (Glascoe Decl. ¶ 16).

After the close of market that day, IMS Health’s stock closed at \$29.56 per share and the trading volume was 832,500 shares. (Gumagay Decl. ¶ 2 and Ex. A). At 4:33 p.m., IMS Health reported third quarter GAAP earnings of \$0.29 per share, which was 28% below the analysts’ consensus estimates of approximately \$0.40 earnings per share and 15% below the previous year’s third quarter earnings of \$0.34 per share. (Gumagay Decl. ¶¶ 8-9 and Exs. G-H).

When the markets opened the following day, October 18, 2007, IMS Health's stock price fell 28% to a low of \$21.20 per share – the steepest decline in the stock's 52-week trading history. (Gumagay Decl. ¶ 2 and Ex. A). Defendant Dorozhko quickly sold all of the 630 IMS Health put options that he had purchased the previous day, and realized proceeds of \$328,571.00 and net profits of \$286,456.59. (Gumagay Decl. ¶ 10 and Ex. I). Dorozhko's trades in IMS Health put options were the first and only trades in his account at Interactive Brokers. (Ward Decl. ¶ 8) Clearly, few besides Defendant Dorozhko anticipated the disappointing earnings. IMS Health's stock closed that day at \$23.12 per share, a decline of approximately 22% from the previous day's closing price. (Gumagay Decl. ¶ 10 and Ex. I). The trading volume was more than 23 million shares, representing a staggering 2,735% increase from the previous day's trading volume. (*Id.*).

Almost immediately, Defendant Dorozhko's broker, concerned that his huge windfall was due to his illegal pre-announcement possession of IMS Health earnings information, froze his account pending the broker's internal investigation of the matter. (Ward Decl. ¶ 14; Hr'g Tr. at 106-108).

On October 29, 2007, the SEC filed an emergency action against Defendant Dorozhko seeking a temporary restraining order freezing assets and granting other relief. That same day, this Court issued the Temporary Restraining Order, An Order Freezing Assets And Granting Other Relief, And An Order To Show Cause Why A Preliminary Injunction Should Not Issue ("Court Order"). Thereafter, Defendant Dorozhko moved, *inter alia*, to dismiss the Complaint for failure to state a claim and for insufficient particularity under Fed. R. Civ. P. Rules 12b(6) and 9(b), and to vacate the Court Order. This Court conducted an evidentiary hearing on

November 28, 2007 and heard oral argument on the motions of the SEC and Defendant Dorozhko.

The primary focus of this brief is to set forth the case law, legal authorities and arguments that sustain the theory that, in the context of the facts at bar, “the hacking of nonpublic material information equals deception in connection with the purchase or sale of securities.” (Hr’g Tr. at 135, lines 8 to 11).

II. RELEVANT PORTIONS OF SECTION 10(b) AND EXCHANGE ACT RULE 10b-5

Section 10(b) of the Exchange Act, 48 Stat. 891, 15 U.S.C. § 78j, prohibits the use in connection with the purchase or sale of any security . . . [of] any . . . deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe.

The SEC has promulgated Rule 10b-5 which provides in pertinent part:

It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange

(a) To employ any device, scheme, or artifice to defraud, [or] . . .

(c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.

17 CFR § 240.10b-5 (1979).³

³ The Rule prohibits ‘any person,’ acting ‘directly or indirectly,’ from employing ‘any device, scheme or artifice to defraud.’ It equally prohibits ‘any act, practice, or course of business which operates as a fraud or deceit upon any person.’ The repeated use of the word ‘any’ evidences Congress’ intention to draft the Rule broadly. See U.S. v. Carpenter, 791 F.2d 1024, 1030 (2d Cir. 1986).

III. DEFENDANT DOROZHKO EMPLOYED THE FRAUDULENT AND DECEPTIVE DEVICE OF "HACKING" TO STEAL IMS HEALTH'S MATERIAL NONPUBLIC INFORMATION AND TO PROFITEER THEREON IN SECURITIES TRADING

The SEC submits that, when Defendant Dorozhko stole material nonpublic information through computer hacking for purposes of gaining an informational advantage in purchasing IMS Health put options, he employed a deceptive device, scheme, or artifice to defraud IMS Health and Thomson Financial "in connection with" the purchase or sale of security and violated Section 10(b) of the Exchange Act and Exchange Act Rule 10b-5. Moreover, this conduct was an act, practice, or course of business that operated as a deceit, if not a fraud, upon IMS Health and Thomson Financial, also in violation of the Statute and Rule.⁴ Reading the Statute and Rule together, to establish a violation under Section 10(b) of the Exchange Act and Exchange Act Rule 10b-5, two elements must be met: (1) the use of a fraudulent device, or any act, practice, or course of business which operates or would operate as a fraud or deceit; (2) "in connection with" the purchase or sale of securities. United States v. O'Hagan, 521 U.S. 642, 651 (1997). We now turn to the first element: the use of a fraudulent or deceptive device.

A. *Computer Hacking Involves Fraud or Deceit as Proscribed by Section 10(b) and Exchange Act Rule 10b-5*

By its very nature, computer hacking involves deceptive or manipulative conduct. The hacker's tricks for gaining access to computers and exploiting information are varied, and include devices such as "eavesdropping and spying," "scanning," "masquerading," "piggybacking and tailgating," "Trojan Horses," "trap doors," "logic bombs," and other

⁴ While the SEC has pled and preserves the alternative facts and arguments that this case may have involved a violation under the classical and misappropriation theories of insider trading, such analysis is unnecessary to reach the above conclusions. The SEC wishes to preserve but not address the issue of tippee liability as it is derivative of the tipper's liability. See, e.g., SEC v. Maio, 51 F.3d 623, 632 (7th Cir. 1995) ("Tippee has a derivative duty not to trade on material nonpublic information when the disclosure of information is improper and the tippee knows or should know that this is the case."). In addition, the SEC has addressed scienter in its earlier brief and the circumstantial evidence developed during the hearing, e.g., the hacking, only adds to the argument that Defendant Dorozhko acted with scienter.

techniques. National Institute of Justice, U.S. Dept of Justice, Computer Crime: Criminal Justice Resource Manual xvi, 9-25 (2d ed.1989) (hereinafter "Criminal Justice Resource Manual") at http://www.eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/22/f5/3e.pdf. Generally, the term "hacking" refers to the illegal or unauthorized access of a computer for exploitation. See Criminal Justice Resource Manual (defining "hacker" as "a person who views and uses computers as objects for exploration and exploitation"); Briggs v. State, 704 A.2d 904, 907 at n.4 (Md. 1998) (defining "hacker" as "synonymous with a computer criminal, and typically refers to a person who breaks into computer networks"); State Wide Photocopy Corp. v. Tokai Fin. Svcs., Inc., 909 F. Supp. 137, 145 (S.D.N.Y. Aug. 3, 1995) (an "electronic trespasser"); see also Blueport Co., LLP v. U.S., 76 Fed. Cl. 702, 704 at n. 6 (Fed. Cl. 2007); Physicians Interactive v. Lathian Systems, Inc., 2003 WL 23018270, *1 at n. 1 (E.D.Va. Dec. 5, 2003) (defining "hack" as "to explore and manipulate the workings of a computer or other technological device or system ... to gain unauthorized access"). A comprehensive definition of "hacking" that delineates all methods of gaining such unauthorized access to computers and taking information from them is elusive, because the technological and creative means of accomplishing such intrusions are in constant evolution. Despite the wide-range of forms it can take, however, the act of hacking is deceptive or fraudulent because it involves employing electronic means to trick, circumvent, or bypass computer security in order to gain unauthorized access to computer systems, networks, and information stored or communicated therein, and to steal such data.

Various federal laws characterize computer hacking as a fraud.⁵ For example, the plain terms of the Computer Fraud and Abuse Act, Title 18, Section 1030 of the U.S. Code prohibit “knowingly and with intent to defraud ... access[ing] a protected computer without authorization ... and obtain[ing] anything of value...” 18 U.S.C. § 1030(a)(4) (2007) (“Fraud and related activity in connection with computers”); see also, 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 1343 (wire fraud); Physicians Interactive, 2003 WL 23018270, *1 at n. 1 (granting a TRO and preliminary injunction under 18 U.S.C. § 1030 because the defendant hacked into a restricted website and rapidly stole and retrieved confidential information).

In the instant case the SEC alleges that Defendant Dorozhko gained illegal access to IMS Health material nonpublic information by tricking and deceiving Thomson Financial’s highly complex computer security system into providing him access as if he were one of those few persons with authorized access. (Hr’g Tr. at 32). Defendant Dorozhko’s deception was intentional and “targeted.” (Hr’g Tr. at 54). He picked a specific date, a specific time, a specific issuer (IMS Health), and a specific source (Thomson Financial) to perpetrate his deception. Defendant Dorozhko’s hacking was highly sophisticated in using computer software and an automated device to deceive Thomson Financial’s system security. (Hr’g Tr. at 46-47). By taking advantage of certain anonymity that is provided by IP addresses, the use of multiple

⁵ While the provisions of the Computer Fraud and Abuse Act, the federal wire fraud, and the federal mail fraud statutes may also provide concurrent jurisdiction over the conduct at bar, Congress has specifically created and delegated principal enforcement responsibilities to the SEC when the misconduct is in connection with securities transactions. See Section 4 of the Exchange Act. For example, in fiscal year 2007 alone, the Commission initiated 262 civil actions, 42 of which sought asset freezes, and 37 of which sought temporary restraining orders. See FY 2007 Annual Report of the U.S. Securities and Exchange Commission, available at <http://www.sec.gov/about/secpar/secpar2007.pdf>. Moreover, the SEC is aggressively combating the relatively new phenomenon of hacking material nonpublic information for purposes of obtaining a trading advantage. See, e.g., SEC v. Lohmus Haavel & Viisemann, et al., 05 CV 9259 (RWS) (S.D.N.Y. Nov. 1, 2005) (settled case against alleged computer hackers trading on material nonpublic information) and SEC v. Blue Bottle Ltd., 07-cv-01380 (CSH) (KNF) (S.D.N.Y. Feb. 26, 2007) (default judgment obtained against alleged computer hackers trading on material nonpublic information).

addresses, and possible “spoofing” of his IP address, he was able to conceal his identity and associations with the deception. (Hr’g Tr. at 53).

B. Established Case Law Supports the SEC’s Position that Theft of Material Nonpublic Information by Hacking “In Connection With” Securities Trading Is Within the Purview of Section 10(b) and Exchange Act Rule 10b-5

The second element for establishing a violation under Section 10(b) of the Exchange Act and Exchange Act Rule 10b-5 is that the fraud or deceit occur “in connection with” the purchase or sale of a security. See O’Hagan, 521 U.S. at 651. In the case at bar, the driving force behind Defendant Dorozhko’s fraudulent and deceptive scheme was to exploit the market value of the stolen material nonpublic information before it became public to quickly engage in securities transactions and thereby secure the economic benefit of his deception. The moment Defendant Dorozhko traded IMS Health securities, he satisfied the second element, that the fraud occur “in connection with the purchase or sale of a security.”

As in O’Hagan, Defendant Dorozhko’s deceptive theft and use of the IMS Health’s material nonpublic information violated Section 10(b) and Rule 10b-5 when he traded. According to the O’Hagan Court, the anti-fraud provisions of the federal securities laws “target[] information of a sort that misappropriators ordinarily capitalize upon to gain no-risk profits through the purchase or sale of securities. Should a misappropriator put such information to other use, the statute’s prohibition would not be implicated. The theory does not catch all conceivable forms of fraud involving confidential information; rather, it catches fraudulent means of capitalizing on such information through securities transactions.” Id. at 656. Here, unlike cash, material nonpublic information derives its value ordinarily from its utility in securities trading. Id. at 657. In sum, Section 10(b) of the Exchange Act and Rule 10b-5 encompass “(1) using *any* deceptive device (2) in connection with the purchase or sale of securities.” O’Hagan, 521 U.S. at 651 (1997) (emphasis added).

IV. SEC'S ACTION AGAINST DEFENDANT DOROZHKO IS CONSISTENT WITH ESTABLISHED LEGAL PRINCIPLES UNDER SECTION 10(b) AND EXCHANGE ACT RULE 10b-5

A. Section 10(b) Addresses Fraud Accomplished Through Hacking

Hacking, unlike theft, is inherently deceptive. Defendant Dorozhko only obtained IMS Health's material nonpublic information through fraudulent means. Specifically, to accomplish his fraud, Defendant Dorozhko used his hacking software to (1) learn that the material nonpublic information had been staged; (2) deceive and trick the Thomson Financial security system into allowing his access to the information as if he were authorized; (3) instantly retrieve copy of the information; and (4) and secretly depart from the compromised Thomson Financial system.

Such conduct constitutes "theft by deception." Model Penal Code §223.3. The offense of "theft by deception," as opposed to simple theft, is the act of purposely obtaining the property of another by deception, where deception is defined as purposely "creating or reinforcing a false impression." *Id.* The Third Circuit has held that theft by deception "involves fraud or deceit." *See Nugent v. Ashcroft*, 367 F.3d 162, 178-79 (3rd Cir. 2004) (addressing the question of whether a conviction for fraud by deceit is a basis for immigration removal proceedings). Moreover, the Eleventh Circuit has recognized that the elements of theft by deception are "materially equivalent" to the elements of establishing mail or wire fraud. *See Kemp v. American Telephone & Telegraph Co.*, 393 F.3d 1354, 1359 (11th Cir. 2004). Thus, Defendant Dorozhko's theft of information by deceiving Thomson Financial's computer systems satisfies the first requirement of Section 10(b) and Exchange Act Rule 10b-5, *i.e.*, that the conduct involves the use of a deceptive device.

B. Chiarella Is Not Inconsistent with Obtaining Information by Deception

The SEC's position in this case is not inconsistent with Chiarella. Chiarella does not stand for the proposition that the only circumstance giving rise to a violation of Section 10(b) is the breach of a duty. What Chiarella held was that in a case alleging that "silence in connection with the purchase or sale of securities" was fraudulent, liability would need to be premised on a "duty to disclose arising from a relationship of trust and confidence" between parties to a transaction. 445 U.S. at 230. But Chiarella did not, of course, address the alternative theories for liability suggested in various concurring and dissenting opinions, because those theories were not presented to the jury and thus could not be considered on appeal. Chiarella v. U.S., 445 U.S. 222, at 236-37 (1980); see also *id.* at 238 (Stevens, J., concurring). In Chiarella, the issue of whether a cognizable duty existed was not presented to the jury and thus could not be considered on appeal. Chiarella v. U.S., 445 U.S. 222, 238 (1980) (Stevens, J., concurring).⁶ Theft by deception also did not go to the jury in Chiarella, nor was it addressed by the majority. It was only the Supreme Court's decision in O'Hagan, seventeen years later, which addressed, and endorsed, the misappropriation theory of liability.

In the instant case, the SEC is pursuing Defendant Dorozhko based on his fraudulent hacking. The fact that Defendant Dorozhko is a stranger to IMS Health and Thomson Financial, and may have no fiduciary or other duties does not preclude the claim. Existing insider trading caselaw, including Chiarella, focuses on finding fraud and deception in the breach of a duty owed

⁶ In their separate opinions, Chief Justice Burger and Justices Blackmun, Brennan, and Marshall concluded that Section 10(b) and Rule 10b-5 establish an obligation to disclose or abstain when a person attempts to trade while in possession of material nonpublic information obtained "not by superior experience, foresight, or industry, but *by some unlawful means*." Chiarella, 445 U.S. at 240 (emphasis added). As Justice Brennan stated, "a person violates § 10(b) whenever he *improperly* obtains or *converts* to his own benefit nonpublic information which he then uses in connection with the purchase or sale of securities." *Id.* at 239 (emphasis added). Indeed, Justices Blackmun and Marshall would go further and hold that, under Exchange Act § 10(b), the mere possession of material nonpublic information that is not available to others precludes trading in the affected securities. Chiarella, 445 U.S. at 251. The SEC does not ask the Court to adopt this interpretation.

because those cases did not factually present the exclusive use of a deceptive device employed as a means of acquiring material nonpublic information. Indeed, the “deceptive acquisition of information” has been deemed to be a deceptive device under Section 10(b) and Exchange Act Rule 10b-5. See SEC v. Rocklage, 470 F.3d 1, 8 (1st Cir. 2006) (also involving misappropriation as breach of a duty). As O’Hagan explains, the federal securities laws protect the integrity of the securities markets against abuses by corporate “outsiders” who gain “access to confidential information that will affect the corporation’s security price when revealed, but who owe no fiduciary or other duty to that corporation’s shareholders.” O’Hagan, 521 U.S. at 653.

C. Even Without the Breach of a Duty, Hacking Is Contemplated as a Violation of Section 10(b) and Exchange Act Rule 10b-5

Many of the cases cited in Defendant Dorozhko’s motion to dismiss are inapposite because they involved an analysis under the classical and misappropriation theories of insider trading. However, the classical and misappropriation theories of insider trading are *only* necessary to establish a violation of Section 10(b) and Rule 10b-5 when the allegations of deception are based on the defendant’s duty, but failure, to disclose certain information prior to trading. See, e.g., Chiarella v. U.S., 445 U.S. 222, 235 (1980) (“When an allegation of fraud is based upon nondisclosure, there can be no fraud absent a duty to speak”). In cases where there was a violation of Section 10(b) and Rule 10b-5 involving the classical or misappropriation theories, the defendants lawfully obtained and held possession of material nonpublic information but committed fraud when they breached their duty either to abstain from trading in the relevant security or to disclose the information or the intent to trade to their principals and any client source of the information. The deception was the failure(s) to make such disclosures before trading. See, e.g., U.S. v. O’Hagan, 521 U.S. 642 (1997) (law firm partner liable under Section 10(b) and Rule 10b-5 for “misappropriating” from his firm and trading securities based on material nonpublic information

concerning a tender offer involving a former client); U.S. v. Falcone, 257 F.3d 226 (2d Cir. 2001) (tippee who received, and traded on, material nonpublic information concerning articles that were to appear on *Business Week* magazine, was found guilty of securities fraud under misappropriation theory); SEC v. Cherif, 933 F.2d 403, 411 (7th Cir. 1991) (defendant breached a continuing duty to his former employer).⁷

Unlike these cases, the basis for the SEC's action against Defendant Dorozhko is his fraudulent and deceptive hacking of IMS Health's material nonpublic information that he used in connection with trading of IMS Health securities. It would be ironic to interpret Section 10(b) of the Exchange Act and Rule 10b-5 to establish liability for trading by an employee or agent of the source of material nonpublic information because of a breach of a fiduciary duty to this source, but not attach liability to a devious and tricky thief such as Dorozhko, who uses a fraudulent and deceptive device to hack into a computer network and steal information for unfair advantage in trading in securities. Interpreting the statute and rule to encompass modern day fraud is entirely consistent with Congressional intent. "To hold otherwise would undermine Congress' ideal in 1934 of 'an open and honest market,' in which superior knowledge in the securities markets would be achieved honestly, fairly, and without resort to pernicious conduct." U.S. v. Carpenter, 791 F.2d 1024, 1036 (2d Cir. 1986) (internal citation omitted); SEC v. Materia, 745 F.2d 197, 203-204 (2d Cir. 1984).

Indeed, two courts in the Southern District of New York have granted temporary restraining orders, preliminary injunctions and asset freezes to the SEC in cases presenting facts

⁷ It is noteworthy that the Seventh Circuit found that actions of the defendant in Cherif "were fraudulent in the common understanding of the word because they deprived some person of something of value by 'trick, deceit, chicane or overreaching.'" Id. at 412 (citing McNally v. United States, 483 U.S. 350, 358 (1987), quoting Hammerschmidt v. United States, 265 U.S. 182, 188 (1924)). The court concluded that it would not, since it did not have to, decide whether, if Cherif were a "mere" thief, *i.e.* not a former employee, his conduct would violate §10(b). Cherif, 933 F.2d at 412. In short, Cherif had facts somewhat similar to those in the case at bar, but, because of a prior employment relationship, the Seventh Circuit ruled on liability based on misappropriation analysis.

that are very similar to the facts in the case at bar involving hacking of material nonpublic information. See, e.g., SEC v. Lohmus Haavel & Viisemann, et al., 05 CV 9259 (RWS) (S.D.N.Y. Nov. 1, 2005) (preliminary injunction and asset freeze ordered Nov. 8, 2005); SEC v. Blue Bottle Ltd., 07-cv-01380 (CSH) (KNF) (S.D.N.Y. Feb. 26, 2007) (preliminary injunction and asset freeze ordered by default March 7, 2007).

While no case has addressed it, at least two academics has endorsed the theory that a hacker who steals material nonpublic information for the purpose of trading on it, violates Exchange Act §10(b) and Rule 10b-5. Robert A. Prentice, The Internet and Its Challenges for the Future of Insider Trading Regulation, 12 Harv.J.L. & Tech, 263, 298-307 (Winter 1999); Donald C. Langevoort, 18 Insider Trading Regulation, Enforcement, and Prevention § 6:14 (Apr. 2007). As Professor Langevoort has noted, “[s]o long as an element of intentional deception was present in the action, the resulting trading would satisfy the ‘in connection with’ requirement and lead to liability under Rule 10b-5. Whether one calls this a misappropriation or not simply is a matter of semantics.” 18 Insider Trading Regulation, Enforcement, and Prevention § 6:14.

To the extent that a duty must exist to establish liability, it may derive from the legal principle of constructive trust. For example, “A person who misappropriates the property of another holds the proceeds of the misappropriation in a constructive trust for the benefit of the innocent owner. The misappropriator is deemed a ‘trustee ex malificio,’...which may be fiduciary status enough to fit within both the misappropriation and abstain or disclose rules even as currently formulated.” Id. at n. 5 (internal citations omitted). It follows that Defendant

Dorozhko owed the duty as constructive trustee of the IMS Health information he stole from IMS Health via Thomson Financial's computer systems.⁸

V. APPLYING SECTION 10(b) AND EXCHANGE ACT RULE 10b-5 TO DEFENDANT DOROZHKO'S CONDUCT COMPORTS WITH CONGRESSIONAL INTENT AND PUBLIC POLICY

Section 10(b)'s legislative history demonstrates that Congress intended to empower the Commission to aggressively pursue new types of fraud and deception in connection with securities transactions. See e.g., Hearings on H.R. 7852 and H.R. 8720 before the House Committee on Interstate and Foreign Commerce, 73d Cong., 2d Sess., 115 (1934) ("[o]f course [section 10(b)] is a catch-all clause to prevent manipulative devices. I do not think there is any

⁸ Additionally, the failure to disclose that one's securities trading is on the basis of stolen material nonpublic information breaches the implied duties of good faith and fair dealing owed to the counter-parties to the transactions. Travelers Intern., A.G. v. Trans World Airlines, Inc., 41 F.3d 1570, 1575 (2d Cir. 1994) ("Under New York law, the implied covenant of good faith and fair dealing inheres in every contract"); Restatement (Second) of Contracts § 205 (1981). The fraudulent effect is particularly palpable in the case of equity option contracts traded on U.S. securities exchanges, where there is an identifiable counter-party with whom the option writer contracts.

The Defendant breached his obligation of good faith and fair dealing.

[I]f the hacker avoids detection and then fails to disclose the information but trades on it instead, there is at least as much "deception" as exists in a misappropriation case as envisioned by Justice Ginsburg in *O'Hagan*. The misappropriation theory has been similarly criticized as based more on a nondeceptive state law breach of fiduciary duty than on the type of deception that typifies a Section 10(b)/Rule 10b-5 violation. However, Justice Ginsburg in *O'Hagan* found sufficient deception in the misappropriator's "feigning fidelity to the source of the information..." Unless the hacker advertises the stolen information before trading on it, which would defeat the purpose of her crime, the hacker is similarly deceiving market participants who do not know of her theft of the inside information.

Prentice, 12 Harvard Journal of Law & Technology at 306.

Moreover, because the put options at issue gave Defendant Dorozhko the sole option to sell his shares to the counter-party, his exercise of such discretion is subject to an obligation of good faith. Travelers Intern., 41 F.3d at 1575. By failing to disclose to the option seller that his purchase was predicated on unlawfully hacked material nonpublic information about the underlying security, Defendant Dorozhko breached his duty of good faith and fair dealing, and thereby also committed securities fraud under Rule 10b-5.

objection to that kind of clause. The Commission should have the authority to deal with new manipulative devices.”).

Moreover, subsequent legislative history of the Insider Trading Sanctions Act of 1984, P.L. No. 98-376, 98 Stat. 1264, substantiates the view that Congress did not intend to limit the scope of Section 10(b) and Exchange Act Rule 10b-5 to only a narrow universe of fraudulent conduct. See H.R. Rep. 98-355, pp. 14-15 (1983), U.S. Code Cong. & Admin. News 1984, p. 2274 (discussing the intent to maintain a broad definition of insider trading and “leaving to the courts the task of analyzing whether all other types of questionable conduct involving illicit misappropriation of market and insider information amounts to a ‘fraudulent act.’”); see also Carpenter, 791 F.2d at 1034 (applying legislative history of the Insider Trading Sanctions Act of 1984 to interpret Section 10(b) in a case of first impression). In enacting the Insider Trading Sanctions Act of 1984, Congress indicated that the intent of the 1934 Act was to condemn all manipulative or deceptive trading “whether the information about a corporation or its securities originates from inside or outside the corporation.” H.R. Rep. No. 98-355, 98th Cong., 1st Sess. 3, 4 (1983), reprinted in [1984] U.S. Code Cong. & Admin. News 2274. According to the Second Circuit, Congress’s rationale for this view was clearly stated: “the abuses sought to be remedied [by section 10(b)] were not limited to actions of corporate insiders and large shareholders.” Carpenter, 791 F.2d at 1030.

Indeed, in construing Section 10(b)’s legislative history in light of Congressional commentary on the Insider Trading Sanctions Act of 1984, the Carpenter court noted that Congress did not intend to limit the field of possible deceptive practices in connection with securities transactions only to those with a particular set of “relationships to corporations or duties to corporations.” Id. at 1031. Rather, Congress sought “to proscribe as well trading on

material, nonpublic information obtained not through skill but through a variety of ‘deceptive’ practices” Id.

Analyzing Defendant Dorozhko’s deceptive practices under Section 10(b) demonstrates that it is precisely the type of fraudulent and deceptive conduct Congress intended to reach with Section 10(b). The question before the Court in the instant case is not whether merely using information unavailable to others gives rise to a Section 10(b) or Rule 10b-5 violation. As noted above in the discussion of Chiarella and as affirmed in Carpenter, that question has been addressed and rejected. See Carpenter, 791 F.2d at 1031 (citing Chiarella, 445 U.S. at 235). Ruling that hacking is a deceptive device and, when done to steal and trade with confidential material information is a violation of §10(b) and Rule 10b-5 will not run afoul of Chiarella’s holding. This matter does not involve mere disparity of knowledge among market participants, but rather an improper advantage obtained through fraud and deceit. Defendant Dorozhko’s deceptive conduct offends the fundamental principles underlying the major securities laws, namely “the promotion of ‘the highest ethical standards . . .’ in every facet of the securities industry.” Carpenter, 791 F.2d at 1031 (quoting SEC v. Capital Gains Research Bureau, 375 U.S. 180, 186-87 (1963)).

To hold that Exchange Act Section 10(b) and Rule 10b-5 do not apply to the facts of this case would mean that Defendant Dorozhko, and subsequent similarly-situated defendants, would escape liability for deceptive practices simply because those particular deceptive practices involved a new technology. Such an overly technical interpretation of Section 10(b) would vitiate the major policy rationales underlying the statute, namely: that “a greater reliance on fraud as a means of competing in the market” which would “reduce overall market participants” and cloud “the perception of fairness and integrity in the securities markets.” H.R. 9233, 73rd

Cong., 2d Sess., Rept. No. 1383 at 7865-66. Indeed, such a position would run afoul of Congress's express concern for preserving fair and open markets. As stated by the Senate Committee on Banking and Currency in enacting the Exchange Act of 1934:

The concept of a free and open market for securities transactions necessarily implies that the buyer and the seller are acting in the exercise of enlightened judgment as to what constitutes a fair price. Insofar as the judgment is warped by false, inaccurate, or incomplete information regarding the corporation, the market price fails to reflect the normal operations of supply and demand.

S. Rep. No. 792, 73rd Cong., 2nd Sess., 3 (1934). Congress's objective of a fair market cannot be achieved where, as in the case at bar, one party to a securities transaction has relied on the deceptive practice of hacking to steal and trade on material nonpublic information unavailable to other market participants. Defendant Dorozhko's 697% return, at the expense of other uninformed market participants, clearly demonstrates the very unfairness Congress sought to deter by enacting §10(b). Glascoe Decl. at ¶ 28. ("Mr. Dorozhko's profits of \$287,346.00 represent a 697% return on his investment.").

Congress created the SEC and gave it primary responsibility to aggressively combat the emerging market-integrity threats such as that presented by the defendant's deceptive practices of hacking and stealing material nonpublic information for the purpose of trading on that information. Without effective enforcement of the federal securities laws, U.S. markets and investors are left defenseless. See, e.g., Hr'g Tr. at 24-25 (Testimony of Timothy Mathias describing damage to Thomson Financial and to investors of a company – such as IMS Health – whose material nonpublic information was hacked and stolen for trading purposes); Hr'g Tr. at 41 (Testimony of Timothy Mathias describing Thomson Financial's lack of authority or tools to trace the identity of the hacker who stole IMS Health's material nonpublic information for trading purposes). As the "government body charged by law with the protection of our financial

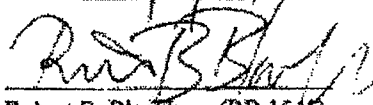
markets,” SEC v. Materia, 745 F.2d 197, 200 (2d Cir. 1984), the SEC is compelled to combat the growing threat of computer theft of material nonpublic information for purposes of securities trading. If investors knew that the SEC and the federal securities laws could not protect the markets against the use of illegally acquired information, and that no amount of research or skill could overcome their informational disadvantage, many would decline to participate in the markets, for they would know that they were playing a game in which the dice might, at any time, be loaded. See O’Hagan, 521 U.S. at 659 (citing Victor Brudney, Insiders, Outsiders, and Informational Advantages Under the Federal Securities Laws, 93 Harv. L. Rev. 322, 356 (1979)). Such a situation is clearly inconsistent with Congress’s intent in prohibiting such deceptive and fraudulent conduct and empowering the Commission to address it through swift and effective litigation such as the case at bar.

VI. CONCLUSION

The SEC has provided evidence and substantial legal authority to show and respectfully request this Court to conclude that the Complaint states a claim for violations of Section 10(b) and Rule 10b-5 with respect to Defendant Dorozhko’s scheme to defraud and use of the deceptive device of hacking to steal and exploit material nonpublic information, not to mention satisfying its burden to warrant the issuance of a preliminary injunction and continuation of the asset freeze.

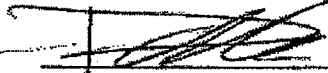
Dated:

12/5/07



Robert B. Blackburn (RB 1545)
Local Counsel
U.S. Securities and Exchange Commission
3 World Financial Center, Room 4300
New York, New York 10281-1022
(212) 336-1050
(212) 336-1317 (Fax)

Respectfully submitted,




Carl A. Tibbetts (Trial Counsel)
Christopher R. Conte
Charles E. Cain
Christine E. Neal
Paul A. Gumagay (PG0805)
Suzanne E. Ashley
Adam J. Eisner
Attorneys for Plaintiff
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, DC 20549-4030
(202) 551-4483 (Tibbetts)
(202) 551-4443 (Gumagay)
(202) 772-9233 (Fax)

CERTIFICATE OF SERVICE

I certify that I served a copy of the foregoing Posthearing Memorandum of Law in Support of Plaintiff Securities and Exchange Commission's Motion For Preliminary Injunction And Other Equitable Relief And Opposition to Defendant Dorozhko's Motion to Dismiss via e-mail and Federal Express for overnight delivery, as indicated below, on December 5, 2007 to the following person at the addresses set forth below:

Charles A. Ross, Esq.
Charles A. Ross & Associates
111 Broadway
Suite 1401
New York, NY 10006
Via Federal Express
& E-mail at cross@carossassoc.com
Counsel to Defendant Dorozhko



Paul A. Gumagay